

FINITE PRIMITIVE GROUPS AND EDGE-TRANSITIVE HYPERGRAPHS

PABLO SPIGA

ABSTRACT. We determine all finite primitive groups that are automorphism groups of edge-transitive hypergraphs. This gives an answer to a problem proposed by Babai and Cameron.

Dedicated in the memory of Ákos Seress

1. INTRODUCTION

A *hypergraph* is a pair $\mathcal{H} = (\Omega, \mathcal{E})$, where Ω is a set and \mathcal{E} is a set of subsets of Ω . The elements of Ω are called *vertices* and the elements of \mathcal{E} are called *edges*. The hypergraph \mathcal{H} is called *r-uniform* if $|E| = r$ for every $E \in \mathcal{E}$, and *uniform* if \mathcal{H} is *r-uniform* for some r . (Clearly, 2-uniform hypergraphs are the usual simple graphs.) Furthermore, \mathcal{H} is *edge-transitive* if the automorphism group $\text{Aut}(\mathcal{H})$ of \mathcal{H} acts transitively on the edges of \mathcal{H} ; observe that every edge-transitive hypergraph is uniform.

Recently Laszlo Babai and Peter Cameron [4, Corollary 1.2] have shown that, for sufficiently large sets Ω , every finite primitive group G on Ω with $G \neq \text{Alt}(\Omega)$ is the automorphism group of an edge-transitive hypergraph, that is, $G = \text{Aut}(\mathcal{H})$ for some edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$. Considering that not every transitive group is the automorphism group of a graph and that rarely a primitive group is the automorphism group of a graph, in our opinion this result comes with considerable surprise. Observe that if $\text{Alt}(\Omega) \leq \text{Aut}(\mathcal{H})$, then $\text{Sym}(\Omega) = \text{Aut}(\mathcal{H})$ and hence $\text{Alt}(\Omega)$ is not the automorphism group of any hypergraph (let alone edge-transitive).

In this paper we refine [4, Corollary 1.2] and we obtain the explicit list of finite primitive groups which are not automorphism groups of edge-transitive hypergraphs.

Theorem 1.1. *Let G be a finite primitive group on Ω with $G \neq \text{Alt}(\Omega)$. Then either there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$, or G is one of the groups in Table 1.*

Deg. 5	$C_5, \text{AGL}_1(5)$
Deg. 6	$\text{PGL}_2(5)$
Deg. 7	$C_7, C_7 \rtimes C_3$
Deg. 8	$\text{AGL}_1(8), \text{AFL}_1(8), \text{PSL}_2(7)$
Deg. 9	$(C_3 \times C_3) \rtimes C_4, \text{AGL}_1(9), (C_3 \times C_3) \rtimes Q_8, \text{ASL}_2(3), \text{PSL}_2(8), \text{PFL}_2(8)$
Deg. 10	$\text{PSL}_2(9), \text{PGL}_2(9)$

TABLE 1. Primitive groups that are not automorphism groups of edge-transitive hypergraphs

Yet again, we find rather surprising that the list of exceptions is so short. The groups $\text{AGL}_1(5)$, $\text{PGL}_2(5)$, $\text{PSL}_2(8)$ and $\text{PFL}_2(8)$ are set-transitive and hence are genuine exceptions in Theorem 1.1: like the alternating group $\text{Alt}(\Omega)$, a proper set-transitive subgroup of $\text{Sym}(\Omega)$ cannot be the automorphism group of any family of subsets of Ω . It is easy to check (for example with the computer algebra system `magnum` [5]) that all the groups in Table 1 are genuine exceptions.

2010 *Mathematics Subject Classification.* 20B15, 20H30.

Key words and phrases. uniform hypergraph, edge-transitive, primitive group, automorphism group of set systems.
Address correspondence to P. Spiga, E-mail: pablo.spiga@unimib.it.

There is a tight analogue between [4, Corollary 1.2] and Theorem 1.1 and two well-known results in the literature. In fact, Cameron, Neumann and Saxl [7] have shown that, apart the alternating and the symmetric group, every finite primitive group on Ω , with $|\Omega|$ sufficiently large, has a regular orbit on the set of subsets of Ω . Later, Seress [19] has computed the explicit list of exceptions. Here the analogy between [7] and [4] and between [19] and Theorem 1.1 is not purely aesthetic: some probabilistic arguments in [4, 7] have a very similar flavour, and we use both the main result and some key ideas in [19] to prove Theorem 1.1.

We observe that (with different terminology) [9, Theorem 4.2] shows that, apart the alternating groups and ten explicit exceptions, every finite primitive group on Ω is the automorphism group of a hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$. The hypergraphs considered in [9] are rather far from being uniform (let alone being edge-transitive) and hence Theorem 1.1 improves [9, Theorem 4.2].

Our proof of Theorem 1.1 requires a detailed knowledge of the structure of the finite primitive groups and in particular we use the O’Nan-Scott theorem combined with the Classification of the Finite Simple Groups.

Acknowledgements. I am in debt with Peter Cameron for suggesting this problem and with the organisers of the conference: “New trends in algebraic combinatorics”, in Villanova, in June 2014. This wonderful environment was extremely fruitful and gave me the opportunity to discover and discuss [4] with Peter.

I am also in debt with Primož Potočnik for hosting the heavy computer computations required in the proof of Theorem 1.1.

1.1. Computer computations. All the computations in this paper are done with the computer algebra system `magma` [5]. These computations require a considerable amount of patience but can be performed with standard built-in `magma` functions.

Given a primitive group G on Ω , we use a “random” approach to exhibit an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$, that is, we generate a random subset Δ of Ω of small cardinality ($|\Delta| \leq 6$) and we check whether $G = \text{Aut}(\Omega, \mathcal{E})$ with $\mathcal{E} = \Delta^G = \{\Delta^g \mid g \in G\}$. Except for the groups in Table 1 (which are not automorphism groups of edge-transitive hypergraphs), typically with this method we succeed with no more than three trials. In particular, this suggests that, for most primitive groups, the proportion of subsets Δ of Ω with $G = \text{Aut}(\Omega, \Delta^G)$ is very large.

Only a handful of cases required a thorough analysis. For instance, $\text{PSL}_3(4)$ in its action on the 21 points of the projective plane of order four is the automorphism group of an edge-transitive 10-uniform hypergraph, but is not the automorphism group of any edge-transitive r -uniform hypergraph for $r \notin \{10, 11\}$.

1.2. Notation. Let Ω be a finite set and let g be a permutation on Ω . We denote by $\text{Fix}_\Omega(g)$ the set $\{\omega \in \Omega \mid \omega^g = \omega\}$, by $\text{fix}_\Omega(g)$ the cardinality $|\text{Fix}_\Omega(g)|$ and by $\text{orb}_\Omega(g)$ the number of cycles of g (in its decomposition in disjoint cycles). Similarly, if C is the cyclic group generated by g , we write $\text{Fix}_\Omega(C) = \text{Fix}_\Omega(g)$, $\text{fix}_\Omega(C) = \text{fix}_\Omega(g)$ and $\text{orb}_\Omega(C) = \text{orb}_\Omega(g)$.

Given a group G , we denote by $\mathcal{C}(G)$ the set of subgroups of prime order of G .

Let G be a primitive group on Ω with $\text{Alt}(\Omega) \not\leq G$. One of the main ingredients in the proof of Theorem 1.1 is the structure of the lattice of overgroups of G : here we will be using the results obtained by Aschbacher in [1, 2] and by Liebeck, Praeger and Saxl in [16, 18]. Following the notation in [1, 2], we denote by $\mathcal{O}(G)$ the lattice $\{M \leq \text{Sym}(\Omega) \mid G \leq M\}$ (ordered by set inclusion) and by $\mathcal{M}(G)$ the maximal elements of $\mathcal{O}(G) \setminus \{\text{Alt}(\Omega), \text{Sym}(\Omega)\}$.

With a slight abuse of terminology and following [4], we say that a subgroup M of $\text{Sym}(\Omega)$ is *maximal* if $M \notin \{\text{Alt}(\Omega), \text{Sym}(\Omega)\}$ and either M is a maximal subgroup of $\text{Sym}(\Omega)$, or $\text{Alt}(\Omega)$ is the only proper subgroup of $\text{Sym}(\Omega)$ containing M . In particular, the elements of $\mathcal{M}(G)$ are exactly the maximal subgroups containing G . From [16], we see that every maximal subgroup has

O’Nan-Scott type HA (“holomorphic abelian”), AS (“almost simple”), PA (“product action”) or SD (“simple diagonal”). Thus, according to this subdivision, we partition the elements of $\mathcal{M}(G)$ in four pair-wise disjoint sets $\mathcal{M}_{\text{HA}}(G)$, $\mathcal{M}_{\text{AS}}(G)$, $\mathcal{M}_{\text{PA}}(G)$ and $\mathcal{M}_{\text{SD}}(G)$.

We denote by $\text{soc}(G)$ the socle of G . Given a subset Δ of Ω , we denote by G_Δ the set-wise stabiliser $\{g \in G \mid \Delta^g = \Delta\}$. We denote by 2^Ω the power-set of Ω , that is, the set of subsets of Ω . Moreover, we define

$$(1) \quad \mathcal{F}(M) = \{\Delta \in 2^\Omega \mid \Delta^g = \Delta \text{ for some } g \in M \setminus \{1\}\}, \text{ and} \\ \mathcal{S}(G) = \bigcup_{M \in \mathcal{M}(G)} \mathcal{F}(M).$$

Thus $\mathcal{F}(M)$ consists of the subsets of Ω fixed by some non-identity element of M and similarly $\mathcal{S}(G)$ consists of the subsets of Ω fixed by some non-identity element of some maximal subgroup containing G .

In this paper, we use the subdivision of the finite primitive groups in eight types as suggested by Laszlo Kovács, and then formulated by Praeger, Liebeck and Saxl (see [17], or [18, Section 3] which has a formulation closer to our application).

2. BASIC LEMMAS

We start with two elementary observations, which are the backbone underlying the idea in the proof of Theorem 1.1.

Lemma 2.1. *Let G be a finite primitive group on Ω with $\text{Alt}(\Omega) \not\leq G$. If $\mathcal{S}(G) \subsetneq 2^\Omega$, then there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$.*

Proof. Let Δ be an element of 2^Ω with $\Delta \notin \mathcal{S}(G)$. Replacing Δ by $\Omega \setminus \Delta$ if necessary, we may assume that $1 \leq |\Delta| \leq |\Omega|/2$. Set $\mathcal{E} = \Delta^G = \{\Delta^g \mid g \in G\}$, $\mathcal{H} = (\Omega, \mathcal{E})$ and $A = \text{Aut}(\mathcal{H})$. By construction \mathcal{H} is an edge-transitive hypergraph and $G \leq A$. Write $n = |\Omega|$ and $m = |\Delta|$.

Suppose that $\text{Alt}(\Omega) \not\leq A$. Then $A \in \mathcal{O}(G) \setminus \{\text{Alt}(\Omega), \text{Sym}(\Omega)\}$ and hence there exists $M \in \mathcal{M}(G)$ with $G \leq A \leq M$. Since $\Delta \notin \mathcal{F}(M)$, we get $M_\Delta = 1$ and hence $A_\Delta = 1$. It follows that

$$|A| = |A : A_\Delta| = |\Delta^A| = |\mathcal{E}| = |\Delta^G| = |G : G_\Delta| = |G|$$

and thus $A = G$.

Suppose that $\text{Alt}(\Omega) \leq A$. (We show that this case cannot occur.) Then $A = \text{Sym}(\Omega)$, $\mathcal{E} = \{\Lambda \in 2^\Omega \mid |\Lambda| = m\}$ and G is transitive on the m -subsets of Ω . As $\Delta \notin \mathcal{S}(G)$, for every $M \in \mathcal{M}(G)$, we get $G_\Delta = M_\Delta = 1$ and hence $|G| = \binom{n}{m} = |M|$. It follows that $\mathcal{M}(G) = \{G\}$ (that is, G is a maximal subgroup of $\text{Sym}(\Omega)$) and G acts regularly on the subsets of Ω of cardinality m . Assume that $m = 1$. Then G acts regularly on Ω and, by primitivity, has prime order. This contradicts the fact that G is maximal. Thus $m \geq 2$. Therefore $|G| = \binom{n}{m} < n!/(n-m)! = n(n-1) \cdots (n-m+1)$ and hence G is not m -transitive. The main result of [12] (see also [10, Theorem 9.4B] for the notation) gives that one of the following happens:

- (i): $m = 2$, $\text{ASL}_1(q) \leq G \leq \text{A}\Sigma\text{L}_1(q)$ with $q \equiv 3 \pmod{4}$;
- (ii): $m = 3$, $\text{PSL}_2(q) \leq G \leq \text{P}\Sigma\text{L}_2(q)$ with $q \equiv 3 \pmod{4}$;
- (iii): $m = 3$, $G \in \{\text{AGL}_1(8), \text{A}\Gamma\text{L}_1(8), \text{A}\Gamma\text{L}_1(32)\}$;
- (iv): $m = 4$, $G \in \{\text{PGL}_2(8), \text{P}\Gamma\text{L}_2(8), \text{P}\Gamma\text{L}_2(32)\}$.

A quick inspection reveals that the groups in this list are either not maximal or do not act regularly on the m -subsets of Ω . This final contradiction concludes the proof. \square

Lemma 2.2. *Let G be a finite primitive group on Ω with $\text{Alt}(\Omega) \not\leq G$. Suppose that $|\mathcal{M}(G)| = 1$. Then either there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$, or G is one of the groups in Table 1.*

Proof. Let M be the maximal subgroup with $\mathcal{M}(G) = \{M\}$. Then $\mathcal{S}(G) = \mathcal{F}(M)$. If $\mathcal{F}(M) \subsetneq 2^\Omega$, then the proof follows from Lemma 2.1. Suppose that $\mathcal{F}(M) = 2^\Omega$, that is, M has no regular orbit on the set of subsets of Ω . Then M is one of the forty-three groups given in [19, Theorem 2] and in particular $5 \leq |\Omega| \leq 17$, or $21 \leq |\Omega| \leq 24$, or $|\Omega| = 32$. Now the proof follows with a case-by-case analysis using the library of small primitive groups in the computer algebra system **magma**. \square

3. PRIMITIVE GROUPS OF HS AND SD TYPE

In this section we prove Theorem 1.1 when G is a primitive group of HS or SD type. This is by far the easiest case to deal with.

Theorem 3.1. *Let G be a finite primitive group on Ω of HS or SD type. Then there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$.*

Proof. Let $M \in \mathcal{M}(G)$. From [18, Proposition 8.1], we have $\text{soc}(M) = \text{soc}(G)$ and hence $M \leq \mathbf{N}_{\text{Sym}(\Omega)}(\text{soc}(G))$. By the maximality of M , we have $M = \mathbf{N}_{\text{Sym}(\Omega)}(\text{soc}(G))$. This shows that $\mathbf{N}_{\text{Sym}(\Omega)}(\text{soc}(G))$ is the unique maximal subgroup of $\text{Sym}(\Omega)$ containing G and $|\mathcal{M}(G)| = 1$. Now the proof follows from Lemma 2.2. \square

Before dealing with other O’Nan-Scott types, we highlight the main ingredients in the proof of Theorem 3.1. First, it is necessary to have a detailed knowledge of all maximal overgroups of G . The work in [1, 2] and in [16, 18] deals with the inclusion problem among primitive groups and is fundamental for our application. Second, it is necessary to establish the existence of a subset Δ of Ω with $M_\Delta = 1$, for every $M \in \mathcal{M}(G)$. Rarely we will be able (as in the proof above) to simply invoke [19, Theorem 2]. However, a probabilistic approach (which is also one of the fundamental tools in [4, 7, 19]) will often reduce this second problem to the case that G has small degree.

4. SOME MORE BASIC LEMMAS AND SOME ESTIMATES

We following four facts can be hardly called lemmas, but they will prove useful.

Lemma 4.1. *Let L be a transitive group of degree ℓ . Then L has at most $\ell^{\log_2(\ell)}$ systems of imprimitivity.*

Proof. Let Δ be the set acted upon by L and let $\delta \in \Delta$. The systems of imprimitivity of L are in one-to-one correspondence with the subgroups of L containing L_δ . Every subgroup U of L with $L_\delta \leq U$ is generated by L_δ and by some right cosets of L_δ , that is, $U = \langle L_\delta, L_\delta x_1, \dots, L_\delta x_v \rangle$ for some right cosets $L_\delta x_1, \dots, L_\delta x_v$ of L . As $|L : L_\delta| = |\Delta| = \ell$, we may choose $v \leq \log_2(\ell)$. It follows that there are at most $\ell^{\log_2(\ell)}$ choices for U . \square

Lemma 4.2. *Let g be a permutation of Ω and let p the smallest prime dividing the order of g . Then $\text{orb}_\Omega(g) \leq (|\Omega| + (p-1)\text{fix}_\Omega(g))/p$ and $2^{\text{orb}_\Omega(g)} = |\{\Delta \in 2^\Omega \mid \Delta^g = \Delta\}|$. In particular, $|\{\Delta \in 2^\Omega \mid \Delta^g = \Delta\}| \leq 2^{(|\Omega| + (p-1)\text{fix}_\Omega(g))/p}$.*

Proof. The element g has cycles of size 1 on $\text{Fix}_\Omega(g)$ and of size at least p on $\Omega \setminus \text{Fix}_\Omega(g)$. Thus $\text{orb}_\Omega(g) \leq |\text{Fix}_\Omega(g)| + |\Omega \setminus \text{Fix}_\Omega(g)|/p = (|\Omega| + (p-1)\text{fix}_\Omega(g))/p$. The rest of the lemma is obvious. \square

Lemma 4.3. *Let M be a permutation group on Ω . Then*

$$|\mathcal{F}(M)| \leq \sum_{C \in \mathcal{C}(M)} 2^{\text{orb}_\Omega(C)} \leq \sum_{C \in \mathcal{C}(M)} 2^{\frac{|\Omega|}{2} + \frac{\text{fix}_\Omega(C)}{2}}.$$

Proof. As $\mathcal{F}(M) = \bigcup_{C \in \mathcal{C}(M)} \{\Delta \in 2^\Omega \mid \Delta^C = \Delta\}$, the proof follows from Lemma 4.2. \square

Let G be a primitive group on Ω and let $M \in \mathcal{M}_{\text{PA}}(G)$ with $M \cong \text{Sym}(m) \text{ wr } \text{Sym}(\ell)$. Then the set Ω admits an M -invariant Cartesian decomposition $\Omega = \Delta_1 \times \cdots \times \Delta_\ell$ with $|\Delta_i| = m \geq 5$ and $\ell \geq 2$. As $G \leq M$, the Cartesian decomposition $\Omega = \Delta_1 \times \cdots \times \Delta_\ell$ is also G -invariant. Conversely, if $\Omega = \Delta_1 \times \cdots \times \Delta_\ell$ is a G -invariant Cartesian decomposition with $|\Delta_i| \geq 5$ and $\ell \geq 2$ then the permutation group $(\text{Sym}(\Delta_1) \times \cdots \times \text{Sym}(\Delta_\ell)) \text{ wr } \text{Sym}(\ell) \cong \text{Sym}(|\Delta_1|) \text{ wr } \text{Sym}(\ell)$ contains G and is maximal (see [16, Theorem]), and hence it belongs to $\mathcal{M}_{\text{PA}}(G)$. Thus we have shown the following.

Lemma 4.4. *Let G be a primitive group on Ω . The elements of $\mathcal{M}_{\text{PA}}(G)$ are in one-to-one correspondence with the G -invariant Cartesian decompositions $\Omega = \Delta_1 \times \cdots \times \Delta_\ell$ with $|\Delta_i| \geq 5$ and $\ell \geq 2$.*

Given a positive integer m and $n = m^2$, we define

$$(2) \quad F_0(n) = 2^{\frac{n}{2} + \frac{\sqrt{n}}{2} + (\sqrt{n}-1) \log_2(\sqrt{n})},$$

$$(3) \quad F'(n) = 2^{n - \frac{11}{2}\sqrt{n} + 8(\log_2(\sqrt{n}))^2 - 4\log_2(\sqrt{n})},$$

$$(4) \quad F''(n) = 2^{n + 2\sqrt{n} \log_2(0.3967) + \sqrt{n}}.$$

Moreover, for every prime number p and for every non-negative integers i and j with $0 < p(i+j) < 11$, we define

$$(5) \quad F_{i,j}^p(n) = \frac{2^{n-(i+j)(p-1)\sqrt{n}+ijp(p-1)} \sqrt{n}!^2}{(p-1)(\sqrt{n}-pi)!(\sqrt{n}-pj)!p^{i+j}i!j!}.$$

Finally, set

$$(6) \quad F(n) = F_0(n) + F'(n) + F''(n) + \sum_{\substack{p \text{ prime}, i,j \geq 0 \\ 0 < p(i+j) < 11}} F_{i,j}^p(n).$$

Observe that each $F_{i,j}^p(n)$ can be written as an elementary function in \sqrt{n} . For example, when $(p, i, j) = (2, 2, 1)$, we have $F_{2,1}^2(n) = 2^{n-3\sqrt{n}+4} \sqrt{n}^2 (\sqrt{n}-1)^2 (\sqrt{n}-2)(\sqrt{n}-3)/16$. In particular, since we have only a handful of triples (p, i, j) with $0 < p(i+j) < 11$, the function $F(n)$ is relatively easy and can be efficiently implemented in a computer.

Lemma 4.5. *Let m and ℓ be positive integers with $m \geq 5$ and $\ell \geq 2$, and let $n = m^\ell$. Let M be the wreath product $\text{Sym}(m) \text{ wr } \text{Sym}(\ell)$ endowed of its natural product action on $\Omega = \Delta^\ell$ with $\Delta = \{1, \dots, m\}$. If $\ell \geq 3$, or if $\ell = 2$ and $m \geq 36$, then $|\mathcal{F}(M)| \leq F(n)$. (The function $F(n)$ is defined in Eq. (6).)*

Proof. Let $B = \text{Sym}(\Delta)^\ell$ be the base group of M . We denote the elements of M by $(h_1, \dots, h_\ell)\sigma$, with $\sigma \in \text{Sym}(\ell)$ and $h_1, \dots, h_\ell \in \text{Sym}(\Delta)$.

Let $g = (h_1, \dots, h_\ell)\sigma \in M$, with $\sigma \neq 1$. We claim that $\text{fix}_\Omega(g) \leq m^{\ell-1}$. Relabelling the index set $\{1, \dots, \ell\}$ if necessary, we may assume that $(1, \dots, k)$ is a non-identity cycle of σ . Let $\omega = (\delta_1, \dots, \delta_\ell) \in \Omega$. Now,

$$\omega^g = (\delta_k^{h_k}, \delta_1^{h_1}, \dots, \delta_{k-2}^{h_{k-2}}, \delta_{k-1}^{h_{k-1}}, \delta'_{k+1}, \dots, \delta'_\ell)$$

for some $\delta'_{k+1}, \dots, \delta'_\ell \in \Delta$. In particular, if $\omega^g = \omega$, then $\delta_1 = \delta_k^{h_k}$, $\delta_2 = \delta_1^{h_1}$, \dots , $\delta_k = \delta_{k-1}^{h_{k-1}}$, that is,

$$\delta_k = \delta_1^{(h_k)^{-1}}, \delta_{k-1} = \delta_1^{(h_{k-1}h_k)^{-1}}, \dots, \delta_2 = \delta_1^{(h_2 \cdots h_{k-1}h_k)^{-1}}.$$

From this we deduce that the first k coordinates of ω are uniquely determined by the first coordinate δ_1 of ω . Therefore $\text{fix}_\Omega(g) \leq m^{\ell-1}$.

Let now $g = (h_1, \dots, h_\ell) \in B$ with $g \neq 1$. An easy computation shows that $\text{fix}_\Omega(g) = \prod_{i=1}^\ell \text{fix}_\Delta(h_i) \leq (m-2)m^{\ell-1}$. Thus, as $m \geq 5$, we have $(m-2)m^{\ell-1} > m^{\ell-1}$ and hence

$\text{fix}_\Omega(g) \leq (m-2)m^{\ell-1}$, for every $g \in M$ with $g \neq 1$. Therefore Lemma 4.3 gives

$$|\mathcal{F}(M)| \leq \sum_{C \in \mathcal{C}(M)} 2^{n-m^{\ell-1}} < 2^{n-m^{\ell-1}} |M| = 2^{n-m^{\ell-1}} m!^\ell \ell!.$$

Assume that $\ell \geq 3$. Using Stirling's formula, with a computation, we get $m! \leq (0.5211 \cdot m)^m$ for $m \geq 5$, and hence

$$\begin{aligned} m!^\ell \ell! &\leq (0.5211 \cdot m)^{m\ell} \ell^{\ell-1} = 2^{m(\log_2(n) + \ell \log_2(0.5211)) + (\ell-1) \log_2(\ell)} \\ &\leq 2^{n^{1/3}(\log_2(n) + 3 \log_2(0.5211)) + 2 \log_2(3)}, \end{aligned}$$

where the last inequality follows with a computation. Another computation gives

$$2^{n-n^{2/3}+n^{1/3}(\log_2(n)+3 \log_2(0.5211))+2 \log_2(3)} < F(n),$$

and hence this concludes the proof when $\ell \geq 3$.

Assume that $\ell = 2$ and $m \geq 36$. Fix c with $0 \leq c \leq m-11$. We use Lemma 4.3 to bound $|\mathcal{F}(M)|$. Let $g = (h_1, h_2)\sigma \in M$ with $\sigma \neq 1$ and with $|g|$ prime. Then $|g| = 2$, $\sigma = (1, 2)$ and $1 = g^2 = (h_1 h_2, h_2 h_1)$, hence $h_2 = h_1^{-1}$ and $g = (h_1, h_1^{-1})\sigma$. Now, an easy computation shows that $\text{Fix}_\Omega(g) = \{(\delta, \delta^{h_1}) \mid \delta \in \Delta\}$, hence $\text{fix}_\Omega(g) = m$ and $2^{\text{orb}_\Omega(g)} = 2^{n/2 + \sqrt{n}/2}$. Since $m! = \sqrt{n}! \leq \sqrt{n}^{\sqrt{n}-1} = 2^{(\sqrt{n}-1) \log_2(\sqrt{n})}$, we get

$$\sum_{C \in \mathcal{C}(M), C \not\leq B} 2^{\text{orb}_\Omega(g)} \leq 2^{\frac{n}{2} + \frac{\sqrt{n}}{2} + (\sqrt{n}-1) \log_2(\sqrt{n})} \stackrel{(\text{see } (2))}{=} F_0(n).$$

We now focus on the subgroups of prime order of B . Given $h \in \text{Sym}(\Delta)$ with $|h| = p$ a prime number, we say that h is of type p^i if h is the product of i cycles of length p . For each prime number p and non-negative integers i, j with $0 < p(i+j) < 11$, define

$$\begin{aligned} \mathcal{C}_{i,j}^p &= \{ \langle (h_1, h_2) \rangle \in \mathcal{C}(M) \mid h_1 \text{ of type } p^i \text{ and } h_2 \text{ of type } p^j \text{ on } \Delta \}, \\ \mathcal{C}' &= \{ \langle (h_1, h_2) \rangle \in \mathcal{C}(M) \mid \langle (h_1, h_2) \rangle \notin \mathcal{C}_{i,j}^p \text{ for every } p, i, j, \text{fix}_\Delta(h_1) \geq c \text{ and } \text{fix}_\Delta(h_2) \geq c \}, \\ \mathcal{C}'' &= \{ \langle (h_1, h_2) \rangle \in \mathcal{C}(M) \mid \text{fix}_\Delta(h_1) < c \text{ or } \text{fix}_\Delta(h_2) < c \}. \end{aligned}$$

Observe that \mathcal{C}' is disjoint from \mathcal{C}'' . Moreover, for every $\langle (h_1, h_2) \rangle \in \mathcal{C}_{i,j}^p$, we have $\text{fix}_\Omega(h_1) = m - pi \geq m - 10$ and $\text{fix}_\Omega(h_2) = m - pj \geq m - 10$. As $c < m - 10$, we get that $\mathcal{C}_{i,j}^p$ is disjoint from \mathcal{C}'' . Thus the sets $\mathcal{C}_{i,j}^p, \mathcal{C}', \mathcal{C}''$ are pair-wise disjoint. Furthermore, every subgroup of prime order of B lies in exactly one of $\mathcal{C}_{i,j}^p, \mathcal{C}', \mathcal{C}''$.

Observe that $\text{Sym}(m)$ contains $\frac{m!}{(m-pi)!p^i i!}$ elements of type p^i and hence

$$|\mathcal{C}_{i,j}^p| = \frac{1}{p-1} \cdot \frac{m!^2}{(m-pi)!(m-pj)!p^{i+j}i!j!}.$$

Given $C \in \mathcal{C}_{i,j}^p$, we have $\text{fix}_\Omega(C) = (m-pi)(m-pj)$ and C has orbits of size p on $\Omega \setminus \text{Fix}_\Omega(C)$. Thus

$$\begin{aligned} \sum_{C \in \mathcal{C}_{i,j}^p} 2^{\text{orb}_\Omega(C)} &= \frac{2^{(m-pi)(m-pj) + \frac{n-(m-pi)(m-pj)}{p}} m!^2}{(p-1)(m-pi)!(m-pj)!p^{i+j}i!j!} \\ &= \frac{2^{n-(i+j)(p-1)m+ij(p^2-p)} m!^2}{(p-1)(m-pi)!(m-pj)!p^{i+j}i!j!} \stackrel{(\text{see } (5))}{=} F_{i,j}^p(n). \end{aligned}$$

Set $\varepsilon = 0.3967$. Using Stirling's formula we get $m! \leq (\varepsilon m)^m$ for $m \geq 36$. Clearly,

$$|\mathcal{C}'| \leq \left(\binom{m}{c} (m-c)! \right)^2 = \left(\frac{m!}{c!} \right)^2 < m^{2(m-c)} = 2^{2(m-c) \log_2(m)}$$

and

$$|\mathcal{C}''| < m!^2 < (\varepsilon m)^{2m} = 2^{2m(\log_2(m) + \log_2(\varepsilon))}.$$

Let C be a subgroup of B of prime order r with $C \notin \bigcup_{i,j,p} \mathcal{C}_{i,j}^p$, and write $C = \langle g \rangle$ with $g = (h_1, h_2)$. We claim that if $C \in \mathcal{C}'$, then $\text{fix}_\Omega(g) \leq m(m-11)$. We argue by contradiction and we assume that $\text{fix}_\Omega(g) > m(m-11)$. Assume that h_1 has type r^x and h_2 has type r^y . As C is not in any of the sets $\mathcal{C}_{i,j}^p$, we have $r(x+y) \geq 11$. Observe that $\text{fix}_\Omega(g) = \text{fix}_\Delta(h_1) \text{fix}_\Delta(h_2) = (m-rx)(m-ry) \leq m(m-rx)$ and hence $rx < 11$. Similarly, $ry < 11$. In particular, we have only a handful of triples (r, x, y) with $r(x+y) \geq 11$, $rx < 11$ and $ry < 11$. By studying each of these triples in turn and using $m \geq 36$, we obtain that the inequality $(m-rx)(m-ry) > m(m-11)$ is never satisfied. We do not give the full argument here, but we simply deal with the case that $(r, x, y) = (2, 3, 3)$ (all the other cases are similar). Now, $(m-rx)(m-ry) = (m-6)^2$ and the inequality $(m-6)^2 > m(m-11)$ hold true only if $36 > m$, a contradiction.

From the previous paragraph it follows that $2^{\text{orb}_\Omega(C)} \leq 2^{n-\frac{11}{2}m}$ when $C \in \mathcal{C}'$. Let C be in \mathcal{C}'' and write $C = \langle g \rangle$ with $g = (h_1, h_2)$. Now, $\text{fix}_\Omega(g) = \text{fix}_\Delta(h_1) \text{fix}_\Delta(h_2) \leq (c-1)m$. Thus $2^{\text{orb}_\Omega(C)} \leq 2^{n/2+(c-1)m/2}$ when $C \in \mathcal{C}''$. Therefore

$$\sum_{C \in \mathcal{C}' \cup \mathcal{C}''} 2^{\text{orb}_\Omega(C)} \leq 2^{n-\frac{11}{2}m+2(m-c)\log_2(m)} + 2^{\frac{n}{2}+\frac{(c-1)m}{2}+2m(\log_2(m)+\log_2(\varepsilon))}.$$

Set $c = \lfloor m-4\log_2(m)+3 \rfloor$ and observe that $c \leq m-11$ for $m \geq 36$. Now, with a careful computation we get

$$\sum_{C \in \mathcal{C}' \cup \mathcal{C}''} 2^{\text{orb}_\Omega(C)} \leq 2^{n-\frac{11}{2}m+8(\log_2(m))^2-4\log_2(m)} + 2^{n+2m\log_2(\varepsilon)+m} \stackrel{(\text{see } (3), (4))}{=} F'(n) + F''(n).$$

Now the proof follows from the definition of $F(n)$. \square

Our choice of c in the proof of Lemma 4.5 is not asymptotically best possible, however it is the formulation that best suits our application.

Let m be a positive integer. Set

$$\begin{aligned} G'(m) &= 2^{\binom{m}{2}-\frac{11}{2}m+33+2(\log_2(m))^2+\log_2(m)}, \\ G''(m) &= 2^{\binom{m}{2}-\frac{1}{2}m+\log_2(0.4)m+(\log_2(m))^2+2\log_2(m)+\frac{3}{4}}. \end{aligned}$$

For every prime number p and positive integer i with $ip < 11$, we set

$$(7) \quad G_i^p(m) = \begin{cases} 2^{\binom{m}{2}-i(p-1)m+\frac{i^2p(p-1)}{2}+\frac{i(p-1)}{2}} \cdot \frac{m!}{(p-1)(m-pi)!p^i i!} & \text{if } p > 2, \\ 2^{\binom{m}{2}-im+i^2+i} \cdot \frac{m!}{(m-2i)!2^i i!} & \text{if } p = 2. \end{cases}$$

Finally, we define

$$(8) \quad G(m) = G'(m) + G''(m) + \sum_{\substack{i \geq 1, p \text{ prime} \\ ip < 11}} G_i^p(m).$$

Lemma 4.6. *Let m be a positive integer with $m \geq 32$ and let M be the symmetric group $\text{Sym}(m)$ in its natural action on the 2-subsets of $\{1, \dots, m\}$. Then $|\mathcal{F}(M)| \leq G(m)$. (The function $G(m)$ is defined in Eq. (8).)*

Proof. We denote by Δ the set $\{1, \dots, m\}$ and by Ω the set of 2-subsets of Δ . Fix c with $c \leq m-11$. For each prime p and positive integer i with $ip < 11$, we set

$$\mathcal{C}_i^p = \{\langle g \rangle \in \mathcal{C}(M) \mid g \text{ has type } p^i \text{ on } \Delta\}.$$

Moreover, define

$$\begin{aligned}\mathcal{C}' &= \{\langle g \rangle \in \mathcal{C}(M) \mid \langle g \rangle \notin \mathcal{C}_i^p \text{ for every } p \text{ and } i, \text{fix}_\Delta(g) \geq c\}, \\ \mathcal{C}'' &= \{\langle g \rangle \in \mathcal{C}(M) \mid \text{fix}_\Delta(g) < c\}.\end{aligned}$$

By construction the sets $\mathcal{C}_i^p, \mathcal{C}', \mathcal{C}''$ are pair-wise disjoint, and $\mathcal{C}(M) = \bigcup_{p,i} \mathcal{C}_i^p \cup \mathcal{C}' \cup \mathcal{C}''$.

Clearly, $|\mathcal{C}_i^p| = m!/((p-1)(m-pi)!p^i i!)$. Moreover, if $C \in \mathcal{C}_i^p$, then $\text{fix}_\Delta(C) = m - pi$, and hence $\text{fix}_\Omega(g) = \binom{m-pi}{2}$ when $p > 2$ and $\text{fix}_\Omega(g) = \binom{m-2i}{2} + i$ when $p = 2$. Hence

$$\text{orb}_\Omega(C) = \begin{cases} \frac{1}{p} \left(\binom{m}{2} - \binom{m-pi}{2} \right) + \binom{m-pi}{2} & \text{when } p > 2, \\ \frac{1}{2} \left(\binom{m}{2} - \binom{m-2i}{2} - i \right) + \binom{m-2i}{2} + i & \text{when } p = 2. \end{cases}$$

Now, an easy computation gives $G_i^p(m) = \sum_{C \in \mathcal{C}_i^p} 2^{\text{orb}_\Omega(C)}$, see (7).

Write $\varepsilon = 0.4$. Observe that $|\mathcal{C}'| \leq \binom{m}{c}(m-c)! = m!/c! < m^{m-c} = 2^{(m-c)\log_2(m)}$ and that $|\mathcal{C}''| < m! < (\varepsilon \cdot m)^m$ for $m \geq 32$.

Let C be in \mathcal{C}' and write $C = \langle g \rangle$. As $C \notin \mathcal{C}_i^p$ for every p and i , we get $\text{fix}_\Delta(g) \leq m-11$ and hence $\text{fix}_\Omega(g) \leq \binom{m-11}{2}$ if $|g| > 2$. If $|g| = 2$, then $\text{fix}_\Delta(g) \leq m-12$ and hence $\text{fix}_\Omega(g) \leq \binom{m-12}{2} + 6$. Now a computation shows that $\binom{m-11}{2} \geq \binom{m-12}{2} + 6$ for $m \geq 18$. In particular, since we are assuming $m \geq 32$, in both cases $\text{fix}_\Omega(C) \leq \binom{m-11}{2}$. It follows that

$$\sum_{C \in \mathcal{C}'} 2^{\text{orb}_\Omega(C)} \leq 2^{\frac{1}{2}\binom{m}{2} + \frac{1}{2}\binom{m-11}{2} + (m-c)\log_2(m)} = 2^{\binom{m}{2} - \frac{11}{2}m + 33 + (m-c)\log_2(m)}.$$

Finally, let $C \in \mathcal{C}''$. Then $\text{fix}_\Delta(C) \leq c-1$ and hence $\text{fix}_\Omega(C) \leq \binom{c-1}{2} + (m-c+1)/2$. It follows that

$$\sum_{C \in \mathcal{C}''} 2^{\text{orb}_\Omega(C)} \leq 2^{\frac{1}{2}\binom{m}{2} + \frac{1}{2}\left(\binom{c-1}{2} + \frac{m-c+1}{2}\right) + m(\log_2(m) + \log_2(\varepsilon))}.$$

Now the lemma follows from the definition of $G(m)$ by taking $c = \lfloor m - 2\log_2(m) \rfloor$ and by a careful computation. \square

5. PRIMITIVE GROUPS OF HC, CD AND TW TYPE

In this section we prove Theorem 1.1 when G is a primitive group on Ω of HC, CD or TW type. This case is already more complicated than the case discussed in Section 3, and presents all the main difficulties (but not the technicalities) of the remaining cases. We start by describing the structure and the action of the groups in these families: this will also set the notation in the proof of Theorem 5.1.

Assume that G is primitive of HC type (respectively, CD type) and let N be the socle of G . Then $G \leq H \text{ wr } L$ for some primitive group H on Δ of HS type (respectively, SD type) and some transitive group L of degree ℓ . Moreover, the action of G on Ω is equivalent to the product action of G on Δ^ℓ . Here N equals the socle of $H \text{ wr } L$, the socle of H is isomorphic to T^a and N is isomorphic to $T^{a\ell}$, for some non-abelian simple group T and some positive integer $a \geq 2$ ($a = 2$ when H is of HS type). Finally, $|\Delta| = |T|^{a-1}$ and $|\Omega| = |T|^{(a-1)\ell}$.

Assume that G is primitive of TW type and let N be the socle of G . Then $G = N \rtimes L$ for some transitive group L of degree ℓ , and $N \cong T^\ell$ for some non-abelian simple group T and some $\ell \geq 6$. The action of G on Ω is equivalent to the natural ‘‘affine’’ action of G on N : the group N acts on the set N by right multiplication and L acts by conjugation. Thus $|\Omega| = |T|^\ell$.

From [18], we get that $\mathcal{M}(G) = \mathcal{M}_{\text{PA}}(G)$ and the elements of $\mathcal{M}(G)$ permutation isomorphic to $\text{Sym}(|\Omega|^{1/\ell'}) \text{ wr } \text{Sym}(\ell')$ (for some divisor ℓ' of ℓ with $\ell' > 1$) are in one-to-one correspondence with the systems of imprimitivity of L with ℓ' blocks of size ℓ/ℓ' . (This correspondence is natural: if L has a system of imprimitivity with ℓ' blocks then the inclusion of L in $\text{Sym}(\ell/\ell') \text{ wr } \text{Sym}(\ell')$

gives rise to a natural inclusion of G in $(H \text{ wr Sym}(\ell/\ell')) \text{ wr Sym}(\ell') \leq \text{Sym}(|\Delta|^{\ell/\ell'}) \text{ wr Sym}(\ell')$. Therefore, by Lemma 4.1, we have

$$(9) \quad |\mathcal{M}(G)| \leq \ell^{\log_2(\ell)}.$$

Theorem 5.1. *Let G be a finite primitive group on Ω of HC, CD or TW type. Then there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$.*

Proof. Write $n = |\Omega|$ and observe that $n \geq |T|^2 \geq 60^2$. We use the notation that we established above. Clearly, $\ell \leq \log_{60}(n)$ and $n^{1/\ell'} \geq \sqrt{n} \geq |T| \geq 60 > 36$, for every divisor ℓ' of ℓ with $\ell' > 1$. Therefore from Eq. (9) and Lemma 4.5, we have

$$|S(G)| \leq \sum_{M \in \mathcal{M}(G)} |\mathcal{F}(M)| \leq |\mathcal{M}(G)| F(n) \leq \log_{60}(n)^{\log_2(\log_{60}(n))} F(n).$$

A computation shows that, for $n \geq 60^2$, the right hand side is strictly smaller than 2^n and hence $S(G) \subsetneq 2^\Omega$. Now the proof follows from Lemma 2.1. \square

6. PRIMITIVE GROUPS OF AS TYPE

In this section we prove Theorem 1.1 when G is a finite primitive group on Ω of AS type. For this proof we use [2, Theorem A].

Definition 6.1. Following [2] (and also [17, 18]), we say that G is *product decomposable* if there exists a finite set Δ , a positive integer ℓ with $\ell \geq 2$, and a subgroup R of $H \text{ wr Sym}(\ell)$ (endowed of its natural product action on Δ^ℓ) such that G is permutation isomorphic to R . Now, [16, Theorem, part II] says that, if G is product decomposable, then one of the following happens:

- (i): $\ell = 2$, $\text{soc}(G) = \text{Alt}(6)$, $|\Delta| = 6$, $|\Omega| = 36$ and G contains an outer-automorphism of $\text{Sym}(6)$,
- (ii): $\ell = 2$, $G = \text{Aut}(M_{12})$, $|\Delta| = 12$ and $|\Omega| = 144$,
- (iii): $\ell = 2$, $\text{soc}(G) = \text{Sp}_4(q)$, $q = 2^k$ for some positive integer $k \geq 2$, $|\Delta| = q^2(q^2 - 1)/2$, $|\Omega| = q^4(q^2 - 1)^2/4$ and G contains a graph automorphism of $\text{Sp}_4(q)$.

The group G is *product indecomposable* if it is not product decomposable.

Theorem 6.2. *Let G be a finite primitive group on Ω of AS type. Then either there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$, or G is one of the groups in Table 1.*

Proof. Let T be the socle of G and let n be the degree of G . Then $T \trianglelefteq G \leq \text{Aut}(T)$.

If $T = \text{PSL}_2(7)$ and $n = 8$, then the proof follows with a computation. In particular, in what follows we may assume that $(T, n) \neq (\text{PSL}_2(7), 8)$. We start by dealing with the case that G is product indecomposable. From [2, Theorem A], we see that one of the following happens:

- (1): $|\mathcal{M}(G)| = 1$;
- (2): $G = T$, $|\mathcal{M}(T)| = 3$, $\text{Aut}(T) \cong \mathbf{N}_{\text{Sym}(\Omega)}(T) \in \mathcal{M}(T)$, $\mathbf{N}_{\text{Sym}(\Omega)}(T)$ is transitive on $\mathcal{M}(T) \setminus \{\mathbf{N}_{\text{Sym}(\Omega)}(T)\}$, and T is maximal in V , where $K \in \mathcal{M}(T) \setminus \{\mathbf{N}_{\text{Sym}(\Omega)}(T)\}$ and $V = \text{soc}(K)$. Further (T, V, n) is one of the following:
 - (a): $(HS, \text{Alt}(m), 15400)$, where $m = 176$ and $n = \binom{m}{2}$,
 - (b): $(G_2(3), \text{P}\Omega_7(3), 3159)$,
 - (c): $(\text{PSL}_2(q), M_n, n)$, where $q \in \{11, 23\}$, $n = q + 1$, and M_n is the Mathieu group of degree n ,
 - (d): $(\text{PSL}_2(17), \text{Sp}_8(2), 136)$;
- (3): $T \cong \text{PSL}_3(4)$ and $n = 280$;
- (4): $T \cong \text{Sz}(q)$, $q = 2^k$, $k \geq 3$ is odd, $n = q^2(q^2 + 1)/2$, $\mathcal{M}(T) = \{K_1, K_2\}$ where $K_i = \mathbf{N}_{\text{Sym}(\Omega)}(V_i) \cong \text{Aut}(V_i)$, $V_1 \cong \text{Alt}(q^2 + 1)$ and the action of V_1 on Ω is equivalent to the action of $\text{Alt}(q^2 + 1)$ on the 2-subsets of $\{1, \dots, q^2 + 1\}$, $V_2 = \text{Sp}_{4k}(2)$, and $\mathbf{N}_{\text{Sym}(\Omega)}(T) \cong \text{Aut}(T)$ is maximal in V_1 ;

(5): $G = \text{PSL}_2(11)$ and $n = 55$.

We deal with each of these possibilities in a case-by-case basis. If Case (1) holds, then the proof follows from Lemma 2.2. If Case (2c), (2d), (3) or (5) holds, then the proof follows with a computation with `magma`.

Suppose that Case (2b) holds. Then $\mathcal{M}(G) = \{K_0, K_1, K_2\}$, with $K_0 \cong \text{Aut}(G_2(3))$ and $K_1 \cong K_2 \cong \text{Aut}(\text{P}\Omega_7(3))$. From [11, Corollary 1], we get that $\text{fix}_\Omega(g) \leq 4n/7$ for every non-identity element g in K_i , for $i \in \{1, 2, 3\}$. It follows from Lemma 4.3 that

$$|\mathcal{S}(G)| \leq |\mathcal{F}(K_0)| + |\mathcal{F}(K_1)| + |\mathcal{F}(K_2)| \leq (|K_0| + |K_1| + |K_2|) \cdot 2^{\frac{n}{2} + \frac{2n}{7}}.$$

A computation shows that $|\mathcal{S}(G)| < 2^n$ and hence $\mathcal{S}(G) \subsetneq 2^\Omega$. Thus the proof follows from Lemma 2.1.

Suppose that Case (2a) holds. Then $\mathcal{M}(G) = \{K_0, K_1, K_2\}$, with $K_0 = \mathbf{N}_{\text{Sym}(\Omega)}(G) \cong \text{Aut}(HS)$ and $K_1 \cong K_2 \cong \text{Sym}(176)$. From [11, Corollary 1], we get that $\text{fix}_\Omega(g) \leq 4n/7$ for every $g \in K_0 \setminus \{1\}$. Therefore, from Lemmas 4.3 and 4.6, we get $|\mathcal{S}(G)| \leq 2^{\frac{n}{2} + \frac{2n}{7}} \cdot |K_0| + 2 \cdot G(176)$. Now a computation shows that $|\mathcal{S}(G)| < 2^n$, hence $\mathcal{S}(G) \subsetneq 2^\Omega$ and we conclude using Lemma 2.1.

Suppose that Case (4) holds. Then $\mathcal{M}(G) = \{K_1, K_2\}$, with $K_1 \cong \text{Sym}(q^2 + 1)$, $K_2 \cong \text{Sp}_{4k}(2)$ and the action of K_1 on Ω is equivalent to the action of $\text{Sym}(q^2 + 1)$ on the 2-subsets of $\{1, \dots, q^2 + 1\}$. From [11, Corollary 1], we get that $\text{fix}_\Omega(g) \leq 4n/7$ for every $g \in K_2 \setminus \{1\}$. Therefore, from Lemmas 4.3 and 4.6, we get $|\mathcal{S}(G)| \leq G(q^2 + 1) + 2^{\frac{n}{2} + \frac{2n}{7}} |K_2|$. Using $q^2 + 1 \geq 65$, a computation shows that $|\mathcal{S}(G)| < 2^n$, hence $\mathcal{S}(G) \subsetneq 2^\Omega$ and we conclude using Lemma 2.1.

Suppose that G is product decomposable. If $T = \text{Alt}(6)$ or $T = M_{12}$, then the proof follows with a computation in `magma`. Therefore we are left with $T = \text{Sp}_4(q)$, $q = 2^k$, $k \geq 2$, $n = (q^2(q^2 - 1)/2)^2$ and G is contained in a wreath product $\text{Sym}(m) \text{wr} \text{Sym}(2)$ with $m = q^2(q^2 - 1)/2$. Here we refer to [16, Section 4] for the information on this permutation representation. From [16, Theorem and Tables III, IV, V], we deduce that $\mathcal{M}_{\text{HA}}(G) = \emptyset$ and $\mathcal{M}_{\text{AS}}(G) = \{K\}$ where $K = \mathbf{N}_{\text{Sym}(\Omega)}(T) \cong \text{Aut}(T)$. We claim that there exists a unique G -invariant Cartesian decomposition of Ω and hence $|\mathcal{M}_{\text{PA}}(G)| = 1$ by Lemma 4.4. Let $\Omega = \Delta_1 \times \Delta_2$ be a G -invariant Cartesian decomposition. The group $T = \text{soc}(G)$ is imprimitive and has two systems of imprimitivity with m blocks of size m (namely, $\{\Delta_1 \times \{\delta\} \mid \delta \in \Delta_2\}$ and $\{\{\delta\} \times \Delta_2 \mid \delta \in \Delta_1\}$), which are interchanged by G . For $\omega = (\delta_1, \delta_2) \in \Omega$, from [16, Section 4], we see that $T_\omega \cong C_{q^2+1} \rtimes C_4$ is the normaliser of a torus of order $q^2 + 1$. Moreover, $T_{\Delta_1 \times \{\delta_2\}} \cong T_{\{\delta_1\} \times \Delta_2} \cong \text{O}_4^-(q) \cong \text{SL}_2(q^2).2 \cong \text{Sp}_2(4).2$ and $T_{\Delta_1 \times \{\delta_2\}}, T_{\{\delta_1\} \times \Delta_2}$ are maximal subgroups of T . From [14, Section 4.8] or the discussion in [16, Section 4], we see that T has exactly two conjugacy classes of subgroups isomorphic to $\text{O}_4^-(q)$: one conjugacy class with representative the stabiliser of a quadratic form for the underlying vector space of T and one with representative the stabiliser of an extension field. These two classes are fixed by the subgroup of index 2 of $\text{Aut}(T)$ consisting of the inner-diagonal and field automorphisms, and are fused by the remaining elements. Furthermore, from the list of maximal subgroups of $\text{Sp}_4(q)$ in [13] (see also [6]), we see that if U is any subgroup of T with $|T : U| = m$, then U is maximal in T and is conjugate to either $T_{\Delta_1 \times \{\delta_2\}}$ or $T_{\{\delta_1\} \times \Delta_2}$. Therefore $\{\Delta_1 \times \{\delta\} \mid \delta \in \Delta_2\}$ and $\{\{\delta\} \times \Delta_2 \mid \delta \in \Delta_1\}$ are the only systems of imprimitivity of T with m blocks of size m and our claim follows. Therefore $\mathcal{M}(G) = \{K, M\}$, where $M \cong \text{Sym}(m) \text{wr} \text{Sym}(2)$. From [11, Corollary 1], we have $\text{fix}_\Omega(g) \leq 4n/7$ for every $g \in K$ with $g \neq 1$. Thus

$$|\mathcal{S}(G)| \leq |\mathcal{F}(K)| + |\mathcal{F}(M)| \leq 2^{\frac{n}{2} + \frac{2n}{7}} |K| + F(n).$$

A computation shows that $|\mathcal{S}(G)| < 2^n$, hence $\mathcal{S}(G) \subsetneq 2^\Omega$ and we conclude using Lemma 2.1. \square

7. PRIMITIVE GROUPS OF HA TYPE

In this section we prove Theorem 1.1 when G is a primitive group on Ω of HA type. We start with a number-theoretic remark.

Lemma 7.1. *Let p be a prime number. Then there are at most $(p-1)/2$ solutions to the equation $p = (q^\ell - 1)/(q - 1)$ where ℓ is a positive integer with $\ell \geq 2$ and q is a prime power.*

Proof. It is clear that if $(q^\ell - 1)/(q - 1) = p = (q'^\ell - 1)/(q' - 1)$, then $q = q'$. Observe that if $(q^\ell - 1)/(q - 1)$ is prime, then ℓ is prime and ℓ divides $p - 1$. Now the proof follows immediately. \square

Lemma 7.1 is far from best possible and should not be taken too seriously. Nevertheless, the equation $p = (q^\ell - 1)/(q - 1)$ can have more than one solution. For instance, $(5^3 - 1)/(5 - 1) = 31 = (2^5 - 1)/(2 - 1)$.

Theorem 7.2. *Let G be a finite primitive group on Ω of HA type. Then either there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$, or G is one of the groups in Table 1.*

Proof. Let V be the socle of G and let H be the stabiliser of a point of Ω . Then V is an elementary abelian p group of size p^d , for some prime number p and some positive integer d . Moreover, $G = V \rtimes H$ and the action of G on Ω is equivalent to the “affine” action of G on V , that is, we may identify G with a subgroup of $\text{AGL}_d(p)$ and H with an irreducible subgroup of $\text{GL}_d(p)$. Write $K = \text{N}_{\text{Sym}(\Omega)}(V)$ and observe that $K \cong \text{AGL}_d(p)$.

From [18], we see that every element of $\mathcal{M}(G)$ is either of HA, PA or AS type, and that $\mathcal{M}_{\text{HA}}(G) = \{K\}$. If $\mathcal{M}(G) = \mathcal{M}_{\text{HA}}(G)$, then the proof follows from Lemma 2.2. Suppose then that $\mathcal{M}_{\text{AS}}(G) \cup \mathcal{M}_{\text{PA}}(G) \neq \emptyset$. Observe that, for every $g \in K$ with $g \neq 1$, we have $\text{fix}_\Omega(g) \leq n/p$ and hence, by Lemma 4.2, $\text{orb}_\Omega(g) \leq n/2 + n/2p = (p+1)n/(2p)$. Therefore

$$(10) \quad |\mathcal{F}(K)| \leq 2^{\frac{(p+1)n}{2p}} |K|.$$

Suppose that $\mathcal{M}_{\text{AS}}(G) \neq \emptyset$ and let $M \in \mathcal{M}_{\text{AS}}(G)$. From [18, Proposition 5.1], we get that either

- (i): $|V| \in \{11, 23, 27\}$, or
- (ii): $|V| = p = (q^\ell - 1)/(q - 1)$ for some prime power q and some $\ell \geq 2$, $M \cong \text{P}\Gamma\text{L}_\ell(q)$ and the action of M on V is equivalent to the natural 2-transitive action of $\text{P}\Gamma\text{L}_\ell(q)$ on the points (or hyperplanes) of the d -dimensional projective space over the finite field of size q .

When Case (i) holds, a computation with **magma** shows that G is the automorphism group of an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$. Then suppose that Case (ii) holds. Since $|\Omega| = |V| = p$ is square-free, $\text{Sym}(\Omega)$ has no primitive subgroups of PA type, that is, $\mathcal{M}_{\text{PA}}(G) = \emptyset$ and $\mathcal{M}(G) = \{K\} \cup \mathcal{M}_{\text{AS}}(G)$. Let M_1, \dots, M_s be representatives for the $\text{Sym}(\Omega)$ -conjugacy classes of the elements of $\mathcal{M}_{\text{AS}}(G)$. Thus $M_i \cong \text{P}\Gamma\text{L}_{\ell_i}(q_i)$, for some $\ell_i \geq 2$ and some prime power $q_i = r_i^{f_i}$, and $(q_i, \ell_i) \neq (q_j, \ell_j)$ when $i \neq j$. Moreover,

$$\mathcal{M}_{\text{AS}}(G) = \bigcup_{i=1}^s \{M_i^g \mid g \in \text{Sym}(\Omega), G \leq M_i^g\}.$$

For each $i \in \{1, \dots, s\}$, write $t_i = |\{M_i^g \mid g \in \text{Sym}(\Omega), G \leq M_i^g\}|$ and let $g_{i,1}, \dots, g_{i,t_i} \in \text{Sym}(G)$ such that

$$\{M_i^g \mid g \in \text{Sym}(\Omega), G \leq M_i^g\} = \{M_i^{g_{i,1}}, \dots, M_i^{g_{i,t_i}}\}.$$

We claim that $t_i \leq (p-1)/(\ell_i f_i)$. Observe that $V^{g_{i,j}^{-1}}$ is a Sylow p -subgroup of M_i , for every j . Therefore, for every j , there exists $a_j \in M_i$ with $V^{g_{i,j}^{-1} a_j} = V$ and hence $g_{i,j} \in M_i \text{N}_{\text{Sym}(\Omega)}(V) = M_i K$. Therefore t_i is at most the number of M_i -cosets contained in $M_i K$, that is, $t_i \leq |M_i K : M_i| = |K : \text{N}_{M_i}(V)| = p(p-1)/(p\ell_i f_i)$ and our claim is proved.

Write

$$m_i = \begin{cases} \frac{4p}{3q_i} & \text{if } \ell_i > 2, \\ \max \left\{ \frac{4p}{3q_i}, 2, q_i^{1/e} + 1 \mid e \text{ divides } f_i, e > 1 \right\} & \text{if } \ell_i = 2. \end{cases}$$

From [15, Theorem 1], we see that for every $g \in M_i$ with $g \neq 1$ we have $\text{fix}_\Omega(g) \leq m_i$ and hence $\text{orb}_\Omega(g) \leq (p + m_i)/2$. It follows that

$$\sum_{M \in \mathcal{M}_{\text{AS}}(G)} |\mathcal{F}(M)| \leq \sum_{i=1}^s 2^{(p+m_i)/2} |M_i| (p-1) / (\ell_i f_i).$$

Now, $|M_i| < p^{\log_2(p)}$, $\ell_i \geq 2$, $m_i \leq \sqrt{p} + 1$ and $s \leq (p-1)/2$ by Lemma 7.1. Using these inequalities and Eq. (10), we get

$$|\mathcal{S}(G)| \leq 2^{(p+1)/2} p(p-1) + 2^{(p+\sqrt{p}+1)/2} p^{\log_2(p)} (p-1)^2 / 4.$$

For $p \geq 139$, a computation (with the help of a computer) shows that the right hand side of this equation is strictly less than 2^p . In particular, when $p \geq 139$, the proof follows from Lemma 2.1. The only primes less than 139 of the form $(q^\ell - 1)/(q - 1)$ with q a prime power and $\ell \geq 2$ are:

$$5, 7, 13, 17, 31, 73, 127.$$

For these values of p we can explicitly construct with **magma** an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ such that $G = \text{Aut}(\mathcal{H})$, except when G is one of the groups in Table 1.

Suppose now that $\mathcal{M}_{\text{AS}}(G) = \emptyset$. Thus $\mathcal{M}(G) = \{K\} \cup \mathcal{M}_{\text{PA}}(G)$ and $\mathcal{M}_{\text{PA}}(G) \neq \emptyset$. In particular, H is an imprimitive linear group. Given $\ell \in \{0, \dots, d\}$, we write

$$\begin{bmatrix} d \\ \ell \end{bmatrix}_p = \frac{(p^d - 1)(p^{d-1} - 1) \cdots (p^{d-\ell+1} - 1)}{(p^\ell - 1)(p^{\ell-1} - 1) \cdots (p - 1)}.$$

From Lemma 4.4, the elements of $\mathcal{M}_{\text{PA}}(G)$ are in one-to-one correspondence with the H -invariant Cartesian decompositions $V = V_1 \times \cdots \times V_\ell$ of V , where $\ell \geq 2$ and $|V_1| = \cdots = |V_\ell| \geq 5$. Let us denote by c_ℓ the number of H -invariant Cartesian decompositions $V = V_1 \times \cdots \times V_\ell$. Observe that, for every $i \in \{1, \dots, \ell\}$, the H -invariant Cartesian decomposition $V = V_1 \times \cdots \times V_\ell$ is uniquely determined by V_i : in fact V_1, \dots, V_ℓ can be reconstructed from the H -orbit of V_i , that is, $\{V_i^h \mid h \in H\} = \{V_1, \dots, V_\ell\}$. This shows that c_ℓ is at most the number of H -orbits of cardinality ℓ in the action on the subspaces of V of dimension d/ℓ , that is,

$$c_\ell \leq \frac{1}{\ell} \begin{bmatrix} d \\ d/\ell \end{bmatrix}_p.$$

Thus

$$|\mathcal{M}_{\text{PA}}(G)| \leq \sum_{\substack{\ell \mid d, \ell > 1 \\ p^{d/\ell} \geq 5}} \frac{1}{\ell} \begin{bmatrix} d \\ d/\ell \end{bmatrix}_p$$

and

$$(11) \quad |\mathcal{S}(G)| \leq 2^{\frac{p+1}{2p}n} \cdot |K| + \sum_{\substack{\ell \mid d, \ell > 1 \\ p^{d/\ell} \geq 5}} \frac{1}{\ell} \begin{bmatrix} d \\ d/\ell \end{bmatrix}_p \mathcal{F}(\text{Sym}(p^{d/\ell}) \text{ wr } \text{Sym}(\ell)).$$

As $|K| = |\text{AGL}_d(p)| < n^{1+\log_2(n)}$ and V has at most $|V|^{d/2}$ subspaces of dimension at most $d/2$, using Lemma 4.5 we get

$$|\mathcal{S}(G)| < 2^{3n/4} \cdot n^{1+\log_2(n)} + n^{\log_2(n)/2} \cdot F(n).$$

A computation gives that the right hand side of this inequality is less than 2^n for $n \geq 10533$. Thus for $n \geq 10533$, we have $\mathcal{S}(G) \subsetneq 2^\Omega$ and we conclude using Lemma 2.1. Similarly, for every p and d with $n = p^d < 10533$, we compute the exact value of the right hand side of Eq. (11) and check when it is strictly less than 2^n . For these values of p and d the proof follows again from Lemma 2.1. The remaining values are: $d = 2$ and $5 \leq p \leq 31$, $d = 3$ and $p \in \{5, 7\}$, $d = 4$ and $p \in \{3, 5\}$, $d = 6$ and $p \in \{2, 3\}$, $d \in \{8, 9, 10\}$ and $p = 2$.

For each of the remaining values of p and d , and for each divisor ℓ of d with $\ell > 1$ and $p^{d/\ell} \geq 5$, we may compute explicitly with a computer the value of

$$\sum_{C \in \mathcal{C}(\text{Sym}(p^{d/\ell}) \text{ wr } \text{Sym}(\ell))} 2^{\text{orb}_\Omega(C)}$$

and use it (in view of Lemma 4.3) as an upper bound for $\mathcal{F}(\text{Sym}(p^{d/\ell}) \text{ wr } \text{Sym}(\ell))$ in Eq. (11). With this improvement we get $|\mathcal{S}(G)| < 2^n$, except when $d = 2$ and $p \in \{5, 7\}$, $d = 4$ and $p = 3$, $d \in \{6, 8\}$ and $p = 2$. Finally each affine primitive group with one of these degrees can be checked directly with `magma`. \square

8. PRIMITIVE GROUPS OF PA TYPE

Finally, in this section we prove Theorem 1.1 when G is a primitive group on Ω of PA type. We start with a preliminary lemma.

Lemma 8.1. *Let G be a finite primitive group of degree n on Ω . Then $|\mathcal{M}_{\text{PA}}(G)| \leq n^{\log_2(n)/2}$.*

Proof. From Lemma 4.4, it suffices to show that Ω admits at most $n^{\log_2(n)/2}$ G -invariant Cartesian decompositions.

Let N be the socle of G . Let $\Omega = \Omega_1 \times \cdots \times \Omega_\ell$ be a G -invariant Cartesian decomposition with $\ell \geq 2$. For each $i \in \{1, \dots, \ell\}$, set

$$\mathcal{C}_i = \{ \{(\omega_1, \dots, \omega_{i-1}, \varepsilon, \omega_{i+1}, \dots, \omega_\ell) \mid \varepsilon \in \Omega_i\} \mid \omega_j \in \Omega_j \text{ for each } j \in \{1, \dots, \ell\} \setminus \{i\} \}.$$

Observe that $\mathcal{C}_1, \dots, \mathcal{C}_\ell$ are systems of imprimitivity for N (with $|\Omega|^{(\ell-1)/\ell}$ blocks of size $|\Omega|^{1/\ell}$) and that G acts transitively on $\{\mathcal{C}_1, \dots, \mathcal{C}_\ell\}$. In particular, $\mathcal{C}_1, \dots, \mathcal{C}_\ell$ (and hence the decomposition $\Omega_1 \times \cdots \times \Omega_\ell$) is uniquely determined by \mathcal{C}_1 because $\mathcal{C}_1^G = \{\mathcal{C}_1^g \mid g \in G\} = \{\mathcal{C}_1, \dots, \mathcal{C}_\ell\}$.

This shows that $|\mathcal{M}_{\text{PA}}(G)|$ is at most the number of systems of imprimitivity for N with blocks of size at most \sqrt{n} . Now the proof follows by the proof of Lemma 4.1. \square

Again, Lemma 8.1 should not be taken too seriously, but it is perfect for our application in the proof of Theorem 8.2.

Theorem 8.2. *Let G be a finite primitive group on Ω of PA type. Then there exists an edge-transitive hypergraph $\mathcal{H} = (\Omega, \mathcal{E})$ with $G = \text{Aut}(\mathcal{H})$.*

Proof. Let N be the socle of G and let n be the cardinality of Ω . Then $N = T_1 \times \cdots \times T_\ell$, where T_1, \dots, T_ℓ are pair-wise isomorphic non-abelian simple groups and $\ell \geq 2$. Moreover, $G \leq H \text{ wr } L$, $\Omega = \Delta^\ell$, H is a primitive group on Δ of AS type with socle isomorphic to T_1 , L is transitive of degree ℓ and the action of G on Ω is the natural product action of G on Δ^ℓ .

Suppose that $(H, |\Delta|) \neq (\text{PSL}_2(7), 8)$ and that H is product indecomposable. Then from [18, Section 7], $\mathcal{M}(G) = \mathcal{M}_{\text{PA}}(G)$ and the elements of $\mathcal{M}_{\text{PA}}(G)$ permutation isomorphic to the wreath product $\text{Sym}(|\Omega|^{1/\ell'}) \text{ wr } \text{Sym}(\ell')$ (for some divisor ℓ' of ℓ with $\ell' > 1$) are in one-to-one correspondence with the systems of imprimitivity of L with ℓ' blocks of size ℓ/ℓ' . (Exactly as in Section 5 for groups of HC, CD and TW type, this correspondence is natural: if L has a system of imprimitivity with ℓ' blocks then the inclusion of L in $\text{Sym}(\ell/\ell') \text{ wr } \text{Sym}(\ell')$ gives rise to a natural inclusion of G in $(H \text{ wr } \text{Sym}(\ell/\ell')) \text{ wr } \text{Sym}(\ell') \leq \text{Sym}(|\Delta|^{\ell/\ell'}) \text{ wr } \text{Sym}(\ell')$.) By Lemmas 4.1 and 4.5, we have $|\mathcal{M}(G)| \leq \ell^{\log_2(\ell)}$ and

$$(12) \quad |\mathcal{S}(G)| \leq \ell^{\log_2(\ell)} F(n).$$

Suppose that ℓ is prime. Then G is contained in a unique maximal subgroup of $\text{Sym}(\Omega)$ (namely $\text{Sym}(\Delta) \text{ wr } \text{Sym}(\ell)$) and the proof follows from Lemma 2.2. In particular, we may assume that $\ell \geq 4$. Observe that $\ell \leq \log_5(n)$. Using this upper bound for ℓ and Eq. (12), it follows that $|\mathcal{S}(G)| < 2^n$ for $n \geq 1290$. Therefore when $n \geq 1290$ we conclude by Lemma 2.1. Assume that $n \leq 1289$. Observe

that $5 \leq |\Delta| = n^{1/\ell} \leq n^{1/4} < 6$ and $1290^{1/5} < 5$. Hence $|\Delta| = 5$, $\ell = 4$ and $N \cong \text{Alt}(5)^4$. Now, the primitive groups of PA type with socle $\text{Alt}(5)^4$ and degree 5^4 can be checked directly with **magma**.

Suppose that $H = \text{PSL}_2(7)$ and $|\Delta| = 8$. Now, from [18, Section 7], $\mathcal{M}(G) = \mathcal{M}_{\text{HA}}(G) \cup \mathcal{M}_{\text{PA}}(G)$. Moreover, since H is product indecomposable, we have $|\mathcal{M}_{\text{PA}}(G)| \leq \ell^{\log_2(\ell)}$ as in the previous case. In particular, when $\ell \geq 3$, Lemma 4.5 gives

$$(13) \quad \sum_{M \in \mathcal{M}_{\text{PA}}(G)} |\mathcal{F}(M)| \leq \ell^{\log_2(\ell)} F(8^\ell).$$

Let $K \in \mathcal{M}_{\text{HA}}(G)$. Then $K \cong \text{AGL}_{3\ell}(2)$ by [18, Proposition 7.1]. As $\text{Sym}(\Omega)$ contains a unique conjugacy class of primitive groups isomorphic to $\text{AGL}_{3\ell}(2)$, we have $\mathcal{M}_{\text{HA}}(G) = \{K^g \mid g \in \text{Sym}(\Omega), G \leq K^g\}$. Write $t = |\mathcal{M}_{\text{HA}}(G)|$. We prove the following inequality:

$$(14) \quad t \leq 16^\ell \frac{|\text{GL}_{3\ell}(2)|}{|\text{GL}_3(2) \text{ wr Sym}(\ell)|} |\text{PGL}_2(7) \text{ wr Sym}(\ell)|.$$

(Observe that the right hand side of Eq. (14) is simply $32^\ell \cdot |\text{GL}_{3\ell}(2)|$.) We argue by contradiction and we assume that Eq. (14) is false. Let $g_1, \dots, g_t \in \text{Sym}(\Omega)$ such that $\mathcal{M}_{\text{HA}}(G) = \{K^{g_1}, \dots, K^{g_t}\}$. In particular, $G^{g_1^{-1}}, \dots, G^{g_t^{-1}} \leq K$ and hence $N^{g_1^{-1}}, \dots, N^{g_t^{-1}} \leq K$. Let V be the socle of K , thus V is an elementary abelian group of order $2^{3\ell}$. As $N^{g_i^{-1}} \cap V \trianglelefteq G^{g_i^{-1}}$, we have $N^{g_i^{-1}} \cap V = 1$ and hence $V N^{g_i^{-1}} \cong V \rtimes N^{g_i^{-1}}$. As $G^{g_i^{-1}} \leq K$, we may identify the $G^{g_i^{-1}}$ -set Ω with V . Thus, since $N^{g_i^{-1}}$ fixes each direct factor of a Cartesian decomposition of Ω , we may write $V = V_1 \times \dots \times V_\ell$ where V_1, \dots, V_ℓ are $N^{g_i^{-1}}$ -invariant subspaces of V of dimension 3. Observe that V has $|\text{GL}_{3\ell}(2) : \text{GL}_3(2) \text{ wr Sym}(\ell)|$ Cartesian decompositions $V = V_1 \times \dots \times V_\ell$ with $\dim V_1 = \dots = \dim V_\ell = 3$. In particular, as Eq. (14) is false, from the pigeon-hole principle there exists a Cartesian decomposition $V = V_1 \times \dots \times V_\ell$ (with $\dim V_i = 3$ for each i) and a subset X of $\{1, \dots, t\}$ such that $|X| > 16^\ell |\text{PGL}_2(7) \text{ wr Sym}(\ell)|$ and $N^{g_x^{-1}}$ fixes each of the subspaces V_1, \dots, V_ℓ for every $x \in X$. Therefore, for every $x, y \in X$, we have $V N^{g_x^{-1}} = V N^{g_y^{-1}}$.

Now, $V N^{g_i^{-1}} = (V_1 T_1^{g_i^{-1}}) \times \dots \times (V_\ell T_\ell^{g_i^{-1}}) \cong \text{AGL}_3(2)^\ell$. A computation shows that $\text{AGL}_3(2)$ contains 16 transitive subgroups isomorphic to $\text{PSL}_2(7)$. Therefore $V N^{g_i^{-1}}$ contains 16^ℓ transitive subgroups isomorphic to $\text{PSL}_2(7)^\ell$. Thus, from the pigeon-hole principle, there exists a subset Y of X such that $|Y| > |\text{PGL}_2(7) \text{ wr Sym}(\ell)|$ and $N^{g_y^{-1}} = N^{g_z^{-1}}$, for every $y, z \in Y$. Fix $y_0 \in Y$. Now, $g_{y_0}^{-1} g_y \in \mathbf{N}_{\text{Sym}(\Omega)}(N)$ for every $y \in Y$. As $|\mathbf{N}_{\text{Sym}(\Omega)}(N)| = |\text{PGL}_2(7) \text{ wr Sym}(\ell)|$, from the pigeon-hole principle we have $g_{y_0}^{-1} g_y = g_{y_0}^{-1} g_z$ for some $y, z \in Y$ with $y \neq z$. Thus $g_y = g_z$, a contradiction. Now Eq. (14) is proved.

Observe that every element of $K \cong \text{AGL}_{3\ell}(2)$ fixes at most $n/2$ points and hence by Lemma 4.3 $|\mathcal{F}(K)| \leq 2^{3n/4} |K|$.

Now, from Eqs. (13) and (14), for $\ell \geq 3$ we get

$$|\mathcal{S}(G)| \leq \sum_{M \in \mathcal{M}(G)} |\mathcal{F}(M)| \leq |\mathcal{F}(K)| |\mathcal{M}_{\text{HA}}(G)| + F(n) |\mathcal{M}_{\text{PA}}(G)| \leq 2^{3n/4} |K| 32^\ell + \ell^{\log_2(\ell)} F(8^\ell).$$

A computation shows that the right hand side of this equation is less than 2^n when $\ell \geq 4$. In particular, when $\ell \geq 4$, we conclude with Lemma 2.1. Finally, the primitive groups of PA type with socle $\text{PSL}_2(7)^2$ (respectively $\text{PSL}_2(7)^3$) and degree 8^2 (respectively 8^3) can be (as usual) checked with **magma**.

Finally suppose that H is product decomposable. Definition 6.1 gives $T_1 \cong \text{Alt}(6)$ and $|\Delta| = 36$, or $T_1 \cong M_{12}$ and $|\Delta| = 144$, or $T_1 \cong \text{Sp}_4(q)$ with $q > 2$ even and $|\Delta| = (q^2(q^2 - 1)/2)^2 \geq (4^2 \cdot (4^2 - 1)/2)^2 = 14400$. From [18, Proposition 7.1] we get $\mathcal{M}(G) = \mathcal{M}_{\text{PA}}(G)$ and from Lemma 8.1 we get $|\mathcal{M}_{\text{PA}}(G)| \leq n^{\log_2(n)/2}$. Thus $|\mathcal{S}(G)| \leq n^{\log_2(n)/2} F(n)$. A computation shows that, for $n \geq 10533$, $n^{\log_2(n)/2} F(n) < 2^n$ and hence for these values of n the proof follows from Lemma 2.1.

Assume that $n < 10533$. As $10533^{1/3} < 36$, we must have $\ell = 2$. Then $|\Delta| < 10533^{1/2}$ and hence $|\Delta| \leq 102$. Thus $(T_1, |\Delta|, \ell, n) = (\text{Alt}(6), 36, 2, 36^2)$. A computation with **magma** shows that Ω has 4 N -invariant Cartesian decompositions. As $4 \cdot F(n) < 2^n$, we conclude again with Lemma 2.1. \square

9. CONCLUDING REMARKS

We finish by bringing together the various threads to prove Theorem 1.1.

Proof of Theorem 1.1. The proof follows immediately from Theorems 3.1, 5.1, 6.2, 7.2 and 8.2. \square

REFERENCES

- [1] M. Aschbacher, Overgroups of primitive groups, *J. Aust. Math. Soc.* **87** (2009), 37–82.
- [2] M. Aschbacher, Overgroups of primitive groups II, *J. Algebra* **322** (2009), 1586–1626.
- [3] L. Babai, The probability of generating the symmetric group, *J. Comb. Theory Ser. A* **52** (1989), 148–153.
- [4] L. Babai, P. J. Cameron, Most primitive groups are full automorphism groups of edge-transitive hypergraphs, arXiv:1404.6739.
- [5] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (3–4) (1997), 235–265.
- [6] J. Bray, D. Holt, C. Roney-Dougall, *The maximal subgroups of the low-dimensional classical groups*, London Mathematical Society Lecture Notes Series **407**, Cambridge University Press, Cambridge, 2013.
- [7] P. J. Cameron, P. M. Neumann, J. Saxl, On groups with no regular orbits on the set of subsets, *Arch. Math.* **43** (1984), 295–296.
- [8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *The Atlas of finite groups*, Clarendon Press, Oxford, 1985.
- [9] F. Dalla Volta, J. Siemons, Orbit equivalence and permutation group defined by unordered relations, *J. Algebr. Comb.* **35** (2012), 547–564.
- [10] J. D. Dixon, B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics **163**, Springer-Verlag, New York, 1996.
- [11] R. Guralnick, K. Magaard, On the minimal degree of a primitive permutation group, *J. Algebra* **207** (1998), 127–145.
- [12] W. M. Kantor, k -homogeneous groups, *Math. Z.* **124**, 261–265.
- [13] P. B. Kleidman, *The subgroup structure of some finite simple groups*, Ph.D. thesis, University of Cambridge, 1987.
- [14] P. Kleidman, M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Notes Series **129**, Cambridge University Press, 1990.
- [15] M. W. Liebeck, J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc. (3)* **63** (1991), 266–314.
- [16] M. W. Liebeck, C. E. Praeger, J. Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111** (1987), 365–383.
- [17] M. W. Liebeck, C. E. Praeger, J. Saxl, On the O’Nan-Scott theorem for finite primitive permutation groups, *J. Austr. Math. Soc.* **44** (1988), 389–396.
- [18] C. E. Praeger, The inclusion problem for finite primitive permutation groups, *Proc. London Math. Soc. (3)* **60** (1990), 68–88.
- [19] Á. Seress, Primitive groups with no regular orbits on the set of subsets, *Bull. London Math. Soc.* **29** (1997), 697–704.

PABLO SPIGA, DIPARTIMENTO DI MATEMATICA E APPLICAZIONI,
 UNIVERSITY OF MILANO-BICOCCA, VIA COZZI 55 MILANO, MI 20125, ITALY
E-mail address: pablo.spiga@unimib.it